In the Claims

Claims remaining in the application are as follows:

1. (Previously presented) A computer-implemented method comprising:

determining whether a source address for a first packet sent by the source address

to a destination address qualifies as a threat, and when the source address

qualifies as the threat, determining whether the destination address is

synthetic;

examining the first packet; and

determining a response to the first packet based upon the examining and based

upon whether the source address qualifies as the threat.

2. (Canceled)

3. (Previously presented) The method of claim 1 further comprising:

when the destination address is determined to be synthetic,

determining the response to be dropping the first packet.

4. (Original) The method of claim 3 further comprising:

dropping the first packet.

5. (Previously presented) The method of claim 1 further comprising:

when the destination address is determined to be not synthetic and the source

address is the threat,

determining whether the source address is on a local network.

6. (Previously Presented) The method of claim 5 further comprising:

when the source address is determined to be not on the local network and the

source address is the threat,

determining that the response is to perform for each respective device of a

plurality of devices on the local network:

selecting the respective device,

creating a respective synthetic hardware address for the respective
device,

creating an address control protocol message comprising the
respective synthetic hardware address as a message source
address,

inserting a corresponding hardware address for a gateway
communicating on behalf of the source address in the address
control protocol message as a message destination hardware
address, and

sending the address control protocol message.

7. (Original) The method of claim 6 further comprising:
performing the response.

8. (Original) The method of claim 6 wherein
the creating the respective synthetic hardware address for the respective device
comprises ensuring that the respective synthetic hardware address is not in
use on the local network.

9. (Original) The method of claim 6 further comprising:
inserting a corresponding logical address for the gateway in the address control
protocol message as a message destination logical address.

10. (Original) The method of claim 6 wherein
the gateway inserts an entry into an address resolution protocol table in response to
receiving the address resolution protocol message, wherein
the entry comprises
the respective synthetic hardware address for the respective device.

11. (Previously Presented) The method of claim 5 further comprising:
when the source address is determined to be on a local network and the source
address qualifies as the threat, determining that the response comprises
creating a synthetic hardware address, and

performing for each respective device of a plurality of devices on the local network:

selecting the respective device,

creating an address control protocol message comprising

the synthetic hardware address as a message source address,

inserting a corresponding hardware address for the respective device in the address control protocol message as a message destination hardware address, and

sending the address control protocol message.

12. (Original) The method of claim 11 further comprising:

performing the response.

13. (Original) The method of claim 11 wherein

the creating the synthetic hardware address comprises ensuring that the synthetic hardware address is not in use on the local network.

14. (Original) The method of claim 11 further comprising:

inserting a corresponding logical address for the respective device in the address control protocol message as a message destination logical address.

15. (Original) The method of claim 11 wherein

the respective device inserts an entry into an address resolution protocol table in response to receiving the address resolution protocol message, wherein the entry comprises

the synthetic hardware address as a source hardware address for the source address.

16. (Previously Presented) The method of claim 5 further comprising:

when the source address is determined to be on the local network and the source address qualifies as the threat,

determining that the response is to perform for each respective device of a plurality of devices on the local network:

selecting the respective device,

creating a respective synthetic hardware address for the respective
device,

creating an address control protocol message comprising

the respective synthetic hardware address as a message
source address,

inserting the source address in the address control protocol message
as a message destination hardware address, and

sending the address control protocol message.

17. (Original) The method of claim 16 further comprising:
performing the response.

18. (Original) The method of claim 16 wherein
the creating the respective synthetic hardware address for the respective device
comprises
ensuring that the respective synthetic hardware address is not in use on the
local network.

19. (Original) The method of claim 16 further comprising:
inserting a corresponding logical address for the source address in the address
control protocol message as a message destination logical address.

20. (Original) The method of claim 16 wherein
the source address inserts an entry into an address resolution protocol table in
response to receiving the address resolution protocol message, wherein
the entry comprises
the respective synthetic hardware address for the respective device.

21. (Original) The method of claim 1 further comprising:
when the source address fails to qualify as the threat,
determining whether the destination address qualifies as a second threat.

22. (Original) The method of claim 21 further comprising:
when the destination address qualifies as the second threat,

determining whether the destination address comprises a synthetic hardware
address, and

when the destination address is a synthetic hardware address,

determining the response to be dropping the first packet.

23. (Original) The method of claim 22 further comprising:
dropping the first packet.

24. (Original) The method of claim 21 further comprising:
when the destination address fails to qualify as the second threat,

determining whether the destination address is a synthetic hardware address,
and

when the destination address is the synthetic hardware address, determining
the response to comprise

modifying the first packet by replacing the destination address with a
hardware address for a device at the destination address; and

sending the first packet.

25. (Original) The method of claim 24 further comprising:
performing the response.

26. (Original) The method of claim 1 further comprising:
when the source address qualifies as the threat,

determining a packet type of the first packet.

27. (Original) The method of claim 26 further comprising:
when the packet type of the first packet is an address resolution protocol request,

determining that the response comprises

creating a reply comprising the destination address as a reply source
address, and sending the reply to the source address.

28. (Original) The method of claim 26 further comprising:
when the packet type of the first packet is an internet common message protocol
echo request, determining that the response comprises

creating a reply to indicate that the destination address is active; and

sending the reply to the source address.

29. (Original) The method of claim 26 further comprising:

when the packet type of the first packet is transmission control protocol,

determining whether the first packet is a transmission control protocol syn request;

when the first packet is the transmission control protocol syn request, determining that the response comprises

creating a transmission control protocol syn response indicating that the source address must receive an acknowledgement for each subsequent packet before the source address can transmit another subsequent packet; and

sending the transmission control protocol syn response to the source address.

30. (Original) The method of claim 26 further comprising:

when the packet type of the first packet is transmission control protocol,

determining whether the first packet is a transmission control protocol syn request;

when the first packet is the transmission control protocol syn request, determining that the response comprises

creating a transmission control protocol syn response comprising a payload; and

sending the transmission control protocol syn response to the source address.

31. (Original) The method of claim 30 wherein

a size of the payload is smaller than a maximum size permitted by a network by which the first packet was transmitted.

32. (Original) The method of claim 26 further comprising:

when the packet type of the first packet is transmission control protocol,

determining whether the first packet is a transmission control protocol window

probe; and

when the first packet is the transmission control protocol window

probe,

determining that the response comprises

creating a transmission control protocol window probe

response comprising a transmission control

protocol window size of zero, and

sending the transmission control protocol window probe

response to the source address.

33. (Original) The method of claim 26 further comprising:

when the packet type of the first packet is transmission control protocol,

determining whether the first packet is a transmission control protocol window

probe;

when the first packet is the transmission control protocol window

probe,

determining that the response comprises

creating a transmission control protocol syn response

comprising a payload; and

sending the transmission control protocol syn response

to the source address.

34. (Original) The method of claim 33 wherein

a size of the payload is smaller than a maximum size permitted by a network by

which the first packet was transmitted.

35. (Original) The method of claim 26 further comprising:

when the packet type of the first packet is transmission control protocol,

determining whether the first packet is a transmission control protocol

acknowledgement; and

when the first packet is the transmission control protocol

acknowledgement, determining that the response comprises

ignoring the first packet.

36. (Original) The method of claim 26 further comprising:

performing the response.

37. (Original) The method of claim 1 wherein

the source address comprises at least one of a logical address and a physical address.

38. (Original) The method of claim 1 wherein

the destination address comprises a logical address.

39. (Original) The method of claim 1 wherein

the examining the first packet comprises examining a header for the first packet.

40. (Original) The method of claim 1 wherein

the examining the first packet does not comprise examining a payload for the first packet.

41. (Canceled)

42. (Currently amended) A system comprising:

tangible computer readable medium with logic instruction means executable by a
 computer processor including:
  threat-determining means for determining whether a source address for a first
   packet sent by the source address to a destination address qualifies
   as a threat;
  synthetic-address-determining means for determining whether the destination
   address is synthetic;
  examining means for examining the first packet; and
  response-determining means for determining a response to the first packet
   based upon the examining and based upon whether the source
   address qualifies as the threat.

43. (Canceled)

44. (Previously presented) The system of claim 42 wherein:

the response-determining means determine the response to be dropping the first
packet when the destination address is synthetic and the source address
qualifies as the threat.

45. (Original) The system of claim 44 further comprising:

dropping means for dropping the first packet.

46. (Original) The system of claim 42 further comprising:

location-determining means for determining whether the source address is on a
local network.

47. (Previously Presented) The system of claim 46 wherein

when the location-determining means determine that the source address is not on
the local network and the source address qualifies as the threat,
the response-determining means are configured to determine that the
response is to perform for each respective device of a plurality of
devices on the local network:
select the respective device,
create a respective synthetic hardware address for the respective
device,
create an address control protocol message comprising
the respective synthetic hardware address as a message
source address,
insert a corresponding hardware address for a gateway
communicating on behalf of the source address in the
address control protocol message as a message
destination hardware address, and
send the address control protocol message.

48. (Previously Presented) The system of claim 46 wherein

when the location-determining means determine that the source address is on the
local network and the source address qualifies as the threat,

the response-determining means are configured to determine that the

response is to

create a synthetic hardware address, and

perform for each respective device of a plurality of devices on the local

network:

select the respective device,

create an address control protocol message comprising

the synthetic hardware address as a message source

address,

insert a corresponding hardware address for the

respective device in the address control protocol

message as a message destination hardware

address, and

send the address control protocol message.

49. (Previously Presented) The system of claim 46 wherein

when the location-determining means determine that the source address is on the

local network and the source address qualifies as the threat,

the response-determining means are configured to determine that the

response is to

perform for each respective device of a plurality of devices on the local

network:

select the respective device,

create a respective synthetic hardware address for the respective

device,

create an address control protocol message comprising

the respective synthetic hardware address as a message

source address,

insert the source address in the address control protocol

message as a message destination hardware address,

and

send the address control protocol message.

50. (Original) The system of claim 42 further comprising:

second threat-determining means for determining whether the destination address
        qualifies as a second threat.

51. (Original) The system of claim 50 further comprising:

second synthetic-address-determining means for determining whether the
        destination address is a synthetic hardware address.

52. (Original) The system of claim 51, wherein

when the second synthetic-address-determining means determine that the
        destination address is
        the synthetic hardware address,
        the response-determining means are configured to determine that the
                response comprises
                modifying the first packet by replacing the destination address with a
                        hardware address for a device at the destination address, and
                sending the first packet.

53. (Original) The system of claim 42 further comprising:

packet-type-determining means for determining a packet type of the first packet.

54. (Original) The system of claim 53 wherein

when the packet-type-determining means determine that the packet type of the first
        packet is an address resolution protocol request,
        the response-determining means are configured to determine that the
                response comprises
                creating a reply comprising the destination address as a reply source
                        address, and
                sending the reply to the source address.

55. (Original) The system of claim 42 further comprising:

performing means for performing the response.

56. (Canceled)

57. (Currently amended) A system comprising:

tangible computer readable medium with logic instruction means executable by a
     computer processor including:

a threat-determining module configured to determine whether a source address for
     a first packet sent by the source address to a destination address qualifies as
     a threat;

a packet-type-determining module configured to determine a packet type of the first
     packet;

an examining module configured to examine the first packet; and

a response-determining module configured to determine a response to the first
     packet based upon the examining and based upon whether the source
     address qualifies as the threat.

58. (Original) The system of claim 57 further comprising:

a synthetic-address-determining module configured to determine whether the
     destination address is synthetic.

59. (Previously Presented) The system of claim 58 wherein:

the response-determining module determines the response to be dropping the first
     packet when the destination address is synthetic and the source address
     qualifies as the threat.

60. (Original) The system of claim 59 further comprising:

a dropping module configured to drop the first packet.

61. (Original) The system of claim 57 further comprising:

a location-determining module configured to determine whether the source address
     is on a local network.

62. (Previously Presented) The system of claim 61 wherein

when the location-determining module determines that the source address is not on
     the local network and the source address qualifies as the threat,

the response-determining module is configured to determine that the
response is to perform for each respective device of a plurality of
devices on the local network:
select the respective device,
create a respective synthetic hardware address for the respective
device,
create an address control protocol message comprising
the respective synthetic hardware address as a message
source address,
insert a corresponding hardware address for a gateway
communicating on behalf of the source address in the
address control protocol message as a message
destination hardware address, and
send the address control protocol message.

63. (Previously Presented) The system of claim 61 wherein
when the location-determining module determines that the source address is on the
local network and the source address qualifies as the threat,
the response-determining means are configured to determine that the
response is to
create a synthetic hardware address, and
perform for each respective device of a plurality of devices on the local
network:
select the respective device,
create an address control protocol message comprising
the synthetic hardware address as a message source
address,
insert a corresponding hardware address for the respective
device in the address control protocol message as a
message destination hardware address, and
send the address control protocol message.

64. (Previously Presented) The system of claim 61 wherein

when the location-determining module determines that the source address is on the

local network and the source address qualifies as the threat,

the response-determining module is configured to determine that the

response is to

perform for each respective device of a plurality of devices on the local

network:

select the respective device,

create a respective synthetic hardware address for the respective

device,

create an address control protocol message comprising

the respective synthetic hardware address as a message

source address,

insert the source address in the address control protocol

message as a message destination hardware address;

and

send the address control protocol message.

65. (Original) The system of claim 57 further comprising:

a second threat-determining module configured to determine whether the

destination address qualifies as a second threat.

66. (Original) The system of claim 57 further comprising:

a second synthetic-address-determining module configured to determine whether

the destination address is a synthetic hardware address.

67. (Original) The system of claim 66, wherein

when the second synthetic-address-determining module determines that the

destination address is the synthetic hardware address,

the response-determining module is configured to determine that the

response comprises

modifying the first packet by replacing the destination address with a

hardware address for a device at the destination address, and

sending the first packet.

68. (Canceled)

69. (Previously presented) The system of claim 57 wherein
when the packet-type-determining module determines that the packet type of the
   first packet is an address resolution protocol request,
   the response-determining module is configured to determine that the
      response comprises
         creating a reply comprising the destination address as a reply source
            address, and
         sending the reply to the source address.

70. (Original) The system of claim 57 further comprising:
a performing module configured to perform the response.

71. (Canceled)

72. (Currently amended) A ~~tangible computer-readable medium~~ <u>computer product</u>
comprising:
<u>logic instruction embedded on computer-readable storage medium executable by a</u>
   <u>computer processor to cause the computer processor to:</u>
~~threat-determining instructions configured to~~ determine whether a source address
   for a first packet sent by the source address to a destination address
   qualifies as a threat;
~~examining instructions configured to~~ examine the first packet;
~~synthetic-address-determining instructions configured to~~ determine whether the
   destination address is synthetic; and
~~response-determining instructions configured to~~ determine a response to the first
   packet based upon the examining and whether the source address qualifies
   as the threat.

73. (Canceled)

Serial No. 10/676,637
June 2, 2008

74. (Currently amended) The ~~computer-readable medium~~ <u>computer product</u> of claim 72 wherein:

the ~~response-determining~~ instructions <u>cause the computer processor to </u>determines~~s~~
      the response to be dropping the first packet when the destination address is
      synthetic and the source address qualifies as the threat.

75. (Currently amended) The ~~computer-readable medium~~ <u>computer product</u> of claim 74 further comprising:

dropping instructions configured to <u>cause the computer processor to </u>drop the first packet.

76. (Currently amended) The ~~computer-readable medium~~ <u>computer product</u> of claim 72 further comprising:

location-determining instructions configured to <u>cause the computer processor to </u>
determine whether the source address is on a local network.

77. (Currently amended) The ~~computer-readable medium~~ <u>computer product</u> of claim 76 wherein

when the location-determining instructions determines that the source address is not
      on the local network and the source address qualifies as the threat,
      the ~~response-determining~~ instructions ~~is configured to~~ <u>cause the computer
            processor to </u>determine that the response is to
            perform for each respective device of a plurality of devices on the local
                network:
            select the respective device,
            create a respective synthetic hardware address for the respective
                device,
            create an address control protocol message comprising
                the respective synthetic hardware address as a message
                    source address,
            insert a corresponding hardware address for a gateway
                communicating on behalf of the source address in the address
                control protocol message as a message destination hardware
                address, and

send the address control protocol message.

78. (Currently amended) The ~~computer-readable medium~~ computer product of claim 76 wherein

when the location-determining instructions determines that the source address is on
     the local network and the source address qualifies as the threat,
     the ~~response-determining means~~ instructions ~~are configured to~~ cause the
          computer processor to determine that the response is to
          create a synthetic hardware address, and
          perform for each respective device of a plurality of devices on the local
               network:
               select the respective device,
               create an address control protocol message comprising
                    the synthetic hardware address as a message source
                        address,
               insert a corresponding hardware address for the respective
                    device in the address control protocol message as a
                    message destination hardware address, and
               send the address control protocol message.

79. (Currently amended) The ~~computer-readable medium~~ computer product of claim 76 wherein

when the location-determining instructions determines that the source address is on
     the local network and the source address qualifies as the threat,
     the ~~response-determining~~ instructions ~~are configured to~~ cause the computer
          processor to determine that the response is to
          perform for each respective device of a plurality of devices on the local
               network:
          select the respective device,
          create a respective synthetic hardware address for the respective
               device,
          create an address control protocol message comprising
               the respective synthetic hardware address as a message
                   source address,

insert the source address in the address control protocol message as
a message destination hardware address, and
send the address control protocol message.

80. (Currently amended) The ~~computer-readable medium~~ computer product of claim
72 further comprising:
second threat-determining instructions configured to determine whether the
destination address qualifies as a second threat.

81. (Currently amended) The ~~computer-readable medium~~ computer product of claim
72 further comprising:
second synthetic-address-determining instructions configured to determine whether
the destination address is a synthetic hardware address.

82. (Currently amended) The ~~computer-readable medium~~ computer product of claim
81, wherein
when the second synthetic-address-determining instructions determine that the
destination address is the synthetic hardware address,
the ~~response-determining~~ instructions ~~is configured to~~ cause the computer
processor to determine that the response comprises
modifying the first packet by replacing the destination address with a
hardware address for a device at the destination address, and
sending the first packet.

83. (Currently amended) The ~~computer-readable medium~~ computer product of claim
72 further comprising:
packet-type-determining instructions configured to determine a packet type of the
first packet.

84. (Currently amended) The ~~computer-readable medium~~ computer product of claim
83 wherein
when the packet-type-determining instructions determines that the packet type of
the first packet is an address resolution protocol request,

the ~~response determining~~ instructions ~~is configured to~~ cause the computer processor to determine that the response comprises

creating a reply comprising the destination address as a reply source address, and

sending the reply to the source address.

85. (Currently amended) The ~~computer-readable medium~~ computer product of claim 72 further comprising:

performing instructions configured to perform the response.

86. (Canceled)